AMENDMENTS TO THE CLAIMS

This listing of claims will replace all prior versions and listings of claims in the application. The listing of claims present each claim with its respective status shown in parentheses.

In the following list, Claim 37 is currently amended. Claims 28-36 and 38-53 remain as previously presented.

Listing of Claims

Claims 1 - 27 Cancelled.

Claim 28 (Previously presented): A method of authenticating a user, the method comprising:

associating the user with a personal communication device possessed by the user;

generating a new password based at least upon a token and a passcode, wherein the token is not known to the user and wherein the passcode is known to the user;

setting a password associated with the user to be the new password;

transmitting the token to the personal communication device; and

receiving the password from the user.

Claim 29 (Previously presented): The method of Claim 28, wherein the new password is generated by concatenating the token and the passcode.

Claim 30 (Previously presented): The method of Claim 28, further comprising receiving a request from the user for the token.

Claim 31 (Previously presented): The method of Claim 30, wherein the request is transmitted by the user through the personal communication device.

Claim 32 (Previously presented): The method of Claim 28, wherein the personal communication device is a mobile phone.

Claim 33 (Previously presented): The method of Claim 28, wherein the personal communication device is a pager.

Claim 34 (Previously presented):   A user authentication system comprising:

a user database configured to associate a user with a personal communication device possessed by the user;

a control module configured to create a new password based at least upon a token and a passcode, wherein the token is not known to the user and wherein the passcode is known to the user, the control module further configured to set a password associated with the user to be the new password;

a communication module configured to transmit the token to the personal communication device; and

an authentication module configured to receive the password from the user.

Claim 35 (Previously presented):   The system of Claim 34, wherein the communication module is further configured to receive a request from the user for the token, and wherein the control module is further configured to create the new password in response to the request.

Claim 36 (Previously presented):   The system of Claim 35, wherein the request is transmitted by the user through the personal communication device.

Claim 37 (Currently Amended):   A method of regulating access to a secure system, the method comprising:

associating [[the]] a user with a personal communication device possessed by the user;

associating the user with an account, wherein an initiation of access through the account requires that the account be activated;

receiving a request transmitted by the personal communication device; and

in response to the receipt of the request, activating the account.

Claim 38 (Previously presented):   The method of Claim 37, further comprising deactivating the account within a predetermined amount of time after the account is activated.

Claim 39 (Previously presented):   The method of Claim 37, wherein an initiation of access through the account further requires that the user supply a valid password.

Claim 40 (Previously presented):   The method of Claim 39, further comprising:

generating a new password based at least upon a token and a passcode, wherein the token is not known to the user and wherein the passcode is known to the user;

setting the valid password to be the new password;

transmitting the token to the personal communication device; and

receiving the valid password from the user.

Claim 41 (Previously presented):   The method of Claim 40, wherein the new password is generated by concatenating the token and the passcode.

Claim 42 (Previously presented):   The method of Claim 40, wherein the token is transmitted in response to the receipt of the request.

Claim 43 (Previously presented):   A method of regulating access to a secure system, the method comprising:

receiving a request for a token, wherein the request is transmitted from a personal communication device as a result of an action by a user;

in response to the receipt of the request, transmitting the token to the personal communication device;

receiving login data from the user in response to a request for authentication information, wherein the login data is based at least upon the token; and

granting access to the secure system based at least upon the received login data.

Claim 44 (Previously presented):   The method of Claim 43, wherein the login data is additionally based upon a passcode known to the user.

Appl. No.   :   09/519,829
Filed   :   March 6, 2000
Office Action Date :   December 15, 2003

Claim 45 (Previously presented): The method of Claim 43, wherein the login data comprises a password.

Claim 46 (Previously presented): The method of Claim 45, wherein the password comprises a passcode and the token, and wherein the passcode is known to the user.

Claim 47 (Previously presented): The method of Claim 46, wherein the password is a concatenation of the passcode and the token.

Claim 48 (Previously presented): The method of Claim 46, wherein the password is a hashed concatenation of the passcode and the token.

Claim 49 (Previously presented): The method of Claim 43, further comprising generating the token.

Claim 50 (Previously presented): An access control system comprising:

a communication module configured to receive a request for a token, wherein the request is transmitted from a personal communication device as a result of an action by a user, and wherein the communication module is further configured to transmit the token to the personal communication device in response to the request;

a user token server configured to generate a valid password based at least upon the token; and

an authentication module configured to receive a submitted password in response to a request for authentication of the user, the authentication module further configured to grant access to the user if at least the submitted password matches the valid password.

Claim 51 (Previously presented): The system of Claim 50, wherein the user token server is further configured to generate the valid password based additionally upon a passcode that is known to the user.

Claim 52 (Previously presented):   The system of Claim 51, wherein the valid password is a concatenation of the passcode and the token.

Claim 53 (Previously presented):   The system of Claim 59, wherein the user token server is further configured to generate the token.